Claims

The invention claimed is:

1. A digital processing method for determining A mod N using a calculating engine having two inputs x and y and which produces an output $x\,y^{-mk}$ mod N, where n is the number of bits in the binary representation of N, where k is the size of the words processed by said engine in bits, and where m is the smallest integer for which $mk \geq n + 2$, said method comprising the steps of:

operating said engine with inputs 1 and A_0 to produce a first result, where A_0 is the low order bits in the representation of A as $A_1\,2^{mk} + A_0$;

adding said first result to A_1 to produce a second result, where the addition is modulo N; and

operating said engine with inputs being said second result and 2^{+2mk} mod N, whereby the output of said engine is A mod N.

2. A digital processing apparatus for determining A mod N, where A is a binary number having the form $A_1\,2^{mk} + A_0$, said apparatus comprising:

a calculating engine having two inputs x and y, and which produces an output $x\,y^{-mk}$ mod N, where n is the number of bits in the binary representation of N, where k is the size of the words processed by said engine in bits, and where m is the smallest integer for which $mk \geq n + 2$;

a register for storing the output from said engine;

a modulo N adder having as a first input the output from said calculating engine or said register, and having said A_1 as a second input;

means for controlling the inputs to said engine over at least two cycles of its operation so as to selectively supply various inputs to said engine, said inputs being selected from the group consisting of the constant *1*, the constant 2^{+2mk}, the output from said register and the output from said adder, said selection operating in sequence so as to produce A mod N in said register.

3. A digital processing method for determining A^B mod N where N is the product of two prime numbers, N_p and N_q, said method comprising the steps of:

determining A_p as A mod N_p;

determining A_q as A mod N_q;

determining B_p as B mod $(N_p - 1)$;

determining B_q as B mod $(N_q - 1)$;

determining A_{pB} as $(A_p)^{B_p}$ mod N_p;

determining A_{qB} as $(A_q)^{B_q}$ mod N_p; and

determining A^B as $A_{qB} + N_q ((A_{pB} - A_{qB}) \bmod N_p)\ U \bmod N_p$, where $U = (1/N_q) \bmod N_p$.

4. The method of claim 3 in which at least one of said first six determining steps is carried out with the use of a calculating engine having two inputs x and y, and which produces an output $x\,y^{-mk}$ mod N, where n is the number of bits in the binary representation of N, where k is the size

of the words processed by said engine in bits, and where m is the smallest integer for which $mk \geq n + 2$.

5. The method of claim 4 in which each one of said first six steps is carried out with the use of said engine.

6. An apparatus for determining $A^B \bmod N$ where N is the product of two prime numbers, N_p and N_q, said apparatus comprising:

a calculating engine having two inputs x and y, and which produces an output $x\,y^{-mk} \bmod N$, where n is the number of bits in the binary representation of N, where k is the size of the words processed by said engine in bits, and where m is the smallest integer for which $mk \geq n + 2$;

a first register for storing A as an input to said engine;

a second register for storing N_p as an input to said engine;

a third register for storing N_q as an input to said engine;

a fourth register for storing $U = (1/N_q) \bmod N_p$ as an input to said engine;

a fifth register for storing $B_q = B \bmod (N_q - 1)$ as an input to said engine;

a sixth register for storing $B_p = B \bmod (N_p - 1)$ as an input to said engine; and

means for storing intermediary results and for controlling the inputs to said engine over a plurality of cycles so that an output of said engine is $A^B \bmod N$.